



Using Notifications

Cisco Unified Operations Manager (Operations Manager) generates alerts in response to events that occur in the IP Telephony environment and the IP fabric. You can view alerts on Operations Manager dashboards, such as the Alerts and Events display. In addition, you can configure notifications to forward information about alerts and events to SNMP trap daemons on other hosts, syslog daemons, and users.

The following topics explain notifications concepts and provide procedures for managing notifications:

- [Understanding Notifications, page 14-1](#)
- [Configuring Event Sets, page 14-4](#)
- [Configuring Notifications, page 14-7](#)
- [Customizing Events, page 14-19](#)

Understanding Notifications

This topic describes how Operations Manager determines when to send a notification and introduces the concepts that you need to be familiar with to configure notifications.



Note

Notifications monitor events on device roles, not on device components. For a list of supported events and the device roles on which they can occur, see [Appendix D, “Events Processed.”](#)

What Causes Operations Manager to Send Notifications?

For each alert or event, Operations Manager compares the event, devices, severity, and state against the configured notification groups and sends a notification when there is a match. Matches can be determined by user-configured event sets and notification criteria. (The procedure for configuring notification criteria is described in [Configuring Notifications, page 14-7.](#))

Operations Manager assigns one severity to each alert or event and changes the state of an alert or event over time, responding to user input and changes on the device. [Table 14-1 on page 14-2](#) lists values for severity and explains how the state of an alert or event changes over time.



Note

You can change event names to names that are more meaningful to you. You can also change the event severity sent in notifications from the Operations Manager default value to a user-defined value. See [Customizing Events, page 14-19.](#)

Table 14-1 *Alert and Event Severity and Status*

Operations Manager categorizes alerts and events by severity and status...	
Severity	Critical Warning Informational
Status	Active—The alert or event is live. Acknowledged—A user has manually acknowledged the alert. A user can acknowledge only active alerts or events. Cleared—The alert or event is no longer active. Note Alerts or events that have been cleared either expire or, if associated with a suspended device, remain in Operations Manager until a user resumes or deletes the device.

What Are Notification Groups?

A notification group is a user-defined set of rules for generating and sending notifications. A notification group includes:

- Notification criterion—A named set of reasons to generate a notification.
- Notification type—The type of notification to send: SNMP trap, e-mail, and syslog.
- Notification recipients—Hostnames and ports for system that listen for SNMP traps or syslog messages; or e-mail addresses.
- Daily subscription activity period—The hours during which Operations Manager should use this subscription while monitoring the alerts and events for which to send notifications.

What Are Notification Criteria?

Notification criteria define what you want to monitor for the purpose of sending notifications. A notification criterion is a user-defined, named set of devices or phones, and alerts and events of a particular severity and status. You must specify notification criteria to configure a notification group.

Operations Manager supports two types of notification criteria:

- Device-Based Criteria—Includes the following:
 - Devices—The devices or device groups that you want to monitor.
 - Event sets—(Optional). One or more groups of events that you want to monitor. See [How Can I Limit Notifications to Those for Specific Events?](#), page 14-4.
 - Alert severity and status—One or more alert severity levels and status.
 - Event severity and status—One or more event severity levels and status.



Note You can also customize the names and severity of the device-based events displayed by Notifications. See [Customizing Events](#), page 14-19.

- Service Quality-Based Criteria—Includes the following:
 - Phones, endpoints, or probes—Phones, call endpoints, or probes that you want to monitor.
 - Alert severity and status—One or more alert severity levels and status.
 - Event severity and status—One or more event severity levels and status.

**Note**

You cannot customize the names and severity of the Service Quality-based events displayed by Notifications.

Service Quality-based criteria are useful when you have purchased a license for Service Monitor and configured Operations Manager as a trap receiver on Service Monitor. Service Quality-based criteria do not include events sets.

For additional information, please see the following topics:

- [Configuring Event Sets, page 14-4](#)
- [Configuring Notifications, page 14-7](#)

What Types of Notifications Can I Send?

Operations Manager provides three types of notification: SNMP trap, e-mail, and syslog. When you configure a notification group, you specify one or more types of notification to send and you must also specify recipients for each type of notification.

SNMP Trap Notifications

Operations Manager generates traps with information about the alert and the events that caused it. CISCO-EPM-NOTIFICATION-MIB defines the trap message format. For more information, see [Appendix C, “Notification MIB.”](#)

**Note**

Using SNMP trap notification is different from forwarding raw traps to another server before they have been processed by Operations Manager. For information about the raw traps that Operations Manager can forward, see [Appendix B, “Pass-Through SNMP Unidentified Traps.”](#)

E-Mail Notifications

Operations Manager generates e-mail messages containing information about the alert and the events that caused it. CISCO-EPM-NOTIFICATION-MIB defines the message, which is included in the e-mail in text format. When you create an e-mail subscription, you can choose whether to include the subject line only or the complete e-mail message.

Syslog Notifications

Operations Manager generates syslog messages that can be forwarded to syslog daemons on remote systems.

**Note**

Syslog messages cannot exceed 1024 bytes. If the syslog message exceeds this limit, it will be truncated to 1024 bytes.

Which Systems and Users Can I Notify?

When you configure a notification group, you must specify recipients for each type of notification:

- **SNMP trap**—Send SNMP traps to a port number on which the host can receive traps. Operations Manager defaults to sending SNMP traps to the port 162. However, you can specify a different port.
- **E-Mail**—Send e-mail to one or more addresses.
- **Syslog**—Send syslog messages to a remote system on which the syslog daemon is configured to listen on a specified port. Operations Manager defaults to sending syslog messages to port 514. However, you can specify a different port.

How Can I Limit Notifications to Those for Specific Events?

In some cases, you might want to send notifications for only a subset of the events that Operations Manager monitors. You can set the events that are of interest to you when you define the notification criterion:

- Specify an event set for a device-based notification criterion. You can create as many events sets as you would like.
- Select the events that you want Operations Manager to monitor for Service Quality-based notification criteria. There are few Service Quality-based events and you can select among them when you add or edit Service Quality-based notification criteria.

Configuring Event Sets

Event sets enable you to group the events the you want Operations Manager to monitor for the purpose of sending notifications.

- Step 1** Select **Notifications > Event Sets**. The Event Set page appears. The Event Set page displays the following information:

GUI Element	Description/Action
Check Box column	Select one check box to edit, delete, or view an event set.
Event Set column	Event set name.
Description column	Event set description.
Add button	Click to add an event set. See Adding and Editing an Event Set, page 14-5 .
Edit button	Click to edit an event set. See Adding and Editing an Event Set, page 14-5 .
Delete button	Click to delete an event set.
View button	Click to view an event set. See Viewing an Event Set, page 14-6 .

You can use event sets to:

- Limit the number of events that Operations Manager notification monitors. When you do not use event sets, Operations Manager notification monitors all events to determine whether to send a notification.
- Aggregate the notifications that you want to send to different destinations. For example, you can create separate event sets for each of the following purposes:
 - Limit the amount of e-mail notification sent to specific individuals or departments to only those for certain events.
 - Write all occurrences of particular events to syslog.
 - Send SNMP traps when certain events occur.

When you create device-based notification criteria, you must include an event set as one of the criteria. The default event set, All_Events, includes all events.

For additional information, please see the following topic:

- [Events Processed, page D-1](#)

Adding and Editing an Event Set

- Step 1** Select **Notifications > Event Sets**. The Event Set page appears, displaying the information in the following table.

GUI Element	Description/Action
Event Set column	Event set name.
Description column	Event set description.

- Step 2** Do one of the following:

- Click **Add**
- Select a check box for an event set and click **Edit**.

Depending on your selection, the **Add Event Set** or **Edit Event Set** page appears.

- Step 3** Edit the information on the page, described in the following table.

GUI Element	Description/Action
Event Set Name field	Event set name—Enter or edit the event set name.
Event Set Description field	Event set description—Optional. Enter a description.
Events table	
Number column	Numbers events serially from one.
Check box column	Select to add an event to the event set. Deselect to remove the event from the event set.
Event column	Event description.

Step 4 Click **OK** to save your changes.

For additional information, please see the following topic:

- [Viewing an Event Set, page 14-6](#)
- [Events Processed, page D-1](#)

Viewing an Event Set

Step 1 Select **Notifications > Event Sets**. The Event Set page appears, displaying the information in the following table.

GUI Element	Description/Action
Event Set column	Event set name.
Description column	Event set description.

Step 2 Select the check box for an event set and click **View**. The Event Set Summary dialog box appears, displaying the following information:

- Event Set Name—User-supplied name.
- Event Set Description—User-supplied description.
- Selected Events—List of events in the event set.

For additional information, please see the following topic:

- [Events Processed, page D-1](#)

Deleting an Event Set

Step 1 Select **Notifications > Event Sets**. The Event Set page appears, displaying the information in the following table.

GUI Element	Description
Event Set column	Event set name.
Description column	Event set description.

- Step 2** Select the check box next to each event set that you want to delete.
- Step 3** Click **Delete**. A confirmation dialog box appears.
- Step 4** Click **Yes** to confirm.
-

For additional information, please see the following topic:

- [Events Processed, page D-1](#)

Configuring Notifications

The Notification Groups page is where notification management activities take place. To open the Notification Groups page, select **Notifications > Notification Criteria**.

These topics explain the activities you can perform from the Notification Groups page:

- [Adding and Editing Device Notification Groups, page 14-10](#)
- [Adding and Editing Service Quality Notification Groups, page 14-13](#)
- [Cloning a Notification Group, page 14-17](#)
- [Viewing Notification Group Configuration Details, page 14-18](#)
- [Deleting Device or Service Quality Notification Groups, page 14-18](#)
- [Suspending a Notification, page 14-18](#)
- [Resuming a Notification, page 14-19](#)

[Figure 14-1](#) shows an example of the Notification Groups page.

Figure 14-1 Notification Groups page

Table 14-2 describes the fields in the Group Administration and Configuration page.

Table 14-2 Fields on the Notification Groups Page

GUI Element	Description/Action
Check box column	Select one check box to edit or delete a notification.
Name column	Notification group name.
Devices/Device Groups	The devices or device groups that are configured for the notification.
Events	The event sets that cause the notification to be sent.
Destinations	<p>The type of notification that will be sent—e-mail, SNMP trap, or syslog message—and the hostnames and e-mail recipients it will be sent to.</p> <p>Note The information shown in the destination box is limited. If the information exceeds the limit, an ellipses (...) is displayed. The complete information will be shown in the tool tip.</p>
Operating Interval	The hours of the day during which the subscription is active.

Table 14-2 *Fields on the Notification Groups Page (continued)*

GUI Element	Description/Action
Status	<p>The notification group status; can be any of the following:</p> <ul style="list-style-type: none"> Active—Operations Manager is using the notification group while monitoring alerts to determine when to send a notification. Suspended—The notification has been manually suspended. Operations Manager will not use the notification group unless you resume it. Inactive—During a period of the day when the notification group is not scheduled to be active.
Filter drop-down menu/Filter button	Enables you to filter what is displayed on the Notifications Group page.
Add > Device-Based Criterion button	Click to add a device notification group. See Adding and Editing Device Notification Groups, page 14-10 .
Add > Service Quality-Based Criterion button	<p>Click to add a Service Quality notification group. See Adding and Editing Service Quality Notification Groups, page 14-13.</p> <p>Note A Service Quality-based criterion is useful only if you have purchased a license for Service Monitor.</p>
Clone button	Starts the process of adding a notification group using a current notification group as a template. See Cloning a Notification Group, page 14-17 .
Edit button	Click to edit a notification criterion. See Adding and Editing Device Notification Groups, page 14-10 and Adding and Editing Service Quality Notification Groups, page 14-13 .
View button	Displays the Notification Group Summary page, where the configuration information for a notification group is displayed.
Suspend button	<ul style="list-style-type: none"> Temporarily stops sending notifications to a host. Temporarily stops sending notifications about a device group. <p>Note Overrides scheduled notification's run time.</p> <p>See Suspending a Notification, page 14-18.</p>
Resume button	<ul style="list-style-type: none"> Start sending notifications to a host again. Start sending notifications about a device group using a previously suspended notification. <p>See Resuming a Notification, page 14-19.</p>
Delete button	Click to delete a notification group. See Deleting Device or Service Quality Notification Groups, page 14-18 .

Adding and Editing Device Notification Groups

This section describes the procedures for adding or editing a device notification group.



Note

You can use existing notification groups as templates for creating new notification groups. For procedures, see [Cloning a Notification Group, page 14-17](#).

Step 1 Select **Notifications > Notification Criteria**.

Step 2 Do one of the following:

- To add a new criterion, click **Add > Device-Based Criterion**.
- To edit an existing criterion, select the check box for a device notification group and click **Edit**.

Depending on your selection, the Add Device-Based Criterion page or Edit Device-Based Criterion page appears.

Step 3 Edit the information on the page, described in the following table.

GUI Element	Description/Action
Device selector pane	Expand device group folders and select check boxes for one or more devices or device groups. Note If you select a device group, the notification criterion will stay up-to-date when devices are added or deleted from Operations Manager <i>only</i> if you also select the Include updates to group membership check box, page 14-11 .
Criterion Name field	Enter a name for the notification criterion.
Customer Identification field	Enter any desired identifying information. If you leave this field empty, it is displayed in notifications as follows: <ul style="list-style-type: none"> In e-mail and syslog notifications, it is left blank. In SNMP trap notifications, it is displayed as follows: Customer ID: -
Customer Revision field	Enter any desired identifying information. If you leave this field empty, it is displayed in notifications as follows: <ul style="list-style-type: none"> In e-mail and syslog notifications, it is left blank. In SNMP trap notifications, it is displayed as follows: Customer Revision: *
Alert Severity check boxes	Select none, one, or more of the following: <ul style="list-style-type: none"> Critical. Warning. Informational.
Alert Status check boxes	Select none, one, or more of the following: <ul style="list-style-type: none"> Active. Acknowledged. Cleared.

GUI Element	Description/Action
Event Set Type list box	Select one.
Event Severity check boxes	Select none, one, or more of the following: <ul style="list-style-type: none"> • Critical. • Warning. • Informational.
Event Status check boxes	Select none, one, or more of the following: <ul style="list-style-type: none"> • Active. • Acknowledged. • Cleared.
Include updates to group membership check box	When selected, if devices are added to or deleted from Operations Manager, the devices are also added to or deleted from the notification criterion. This happens when the notification criterion includes a device group that the devices belong to. Deselect to maintain a static list of devices for any device groups included in the notifications criterion.

Step 4 Click **Next**. The Destination: Edit Device Criteria page appears.

Step 5 Edit the information on this page as described in the following table.

GUI Element	Description/Action
Always Active check box	Schedules the notification group to always be active.
Active From: To: fields	Select the hours of the day during which you want this notification group to be active: <ul style="list-style-type: none"> • From: HH:MM—Select hour and minute that the subscription becomes active. • To: HH:MM—Select the last hour and minute during which the subscription is active. <p>By default, the values are from 00:00 to 00:00 and the subscription is active for 24 hours.</p> <p>Note Use this field, for example, to send e-mail notifications to a pager during one shift and not during another.</p>
Include Link to Notification Details check box	Select to include URLs in the notification from which users can directly open the relevant page in Operations Manager for more information. Deselect to omit URLs from notifications.

GUI Element	Description/Action
Subscription Type radio buttons	<p>Select one at a time to enter data for each subscription type that you want to include in this subscription:</p> <ul style="list-style-type: none"> Trap—Enter data in the Trap Subscription Type fields, page 14-12. E-Mail—Enter data in the E-Mail Subscription Type fields, page 14-12. Syslog—Enter data in the Syslog Subscription Type fields, page 14-12. <p>Note Operations Manager does not save the data you enter until you click Finish on the Subscription: Summary page. To go to the Subscription: Summary page, click Next.</p>
Trap Subscription Type fields	
Hostname editable column	Enter an IP address or DNS name for the host.
Port editable column	Enter a port number on which the host can receive traps. If the port number is left unspecified (empty), the port defaults to 162.
Comments editable column	(Optional) Enter a comment.
E-Mail Subscription Type fields	
SMTP Server field	<p>Enter a fully qualified DNS name or IP address for a Simple Mail Transfer Protocol (SMTP) server. (The name of the default SMTP server might already be displayed.)</p> <p>Note To select from any nondefault SMTP servers in use by existing subscriptions, click the SMTP Servers button.</p> <p>Note For instructions on how to configure a default SMTP server, see the Setting System-Wide Parameters Using System Preferences, page 19-12.</p>
Sender Address field	Enter the e-mail address that notifications should be sent from. If the sender's e-mail service is hosted on the SMTP server specified, you need enter only the username. You do not need to enter the domain name.
Recipient Address(es) field	<p>Enter one or more e-mail addresses that notifications should be sent to, separating multiple addresses with either a comma or a semicolon.</p> <p>If a recipient's e-mail service is hosted on the SMTP server specified, you need to enter only the username. You do not need to enter the domain name.</p>
Subject Only check box	<p>Select to include only the subject in the e-mail message.</p> <p>Deselect to send a fully detailed e-mail message (default).</p>
Syslog Subscription Type fields	

GUI Element	Description/Action
Facility list	<p>Select a facility from the list (the default is Local Use 0). The Facility field and the event/alert severity are used for the PRI portion of the syslog message, as follows:</p> <p style="text-align: center;"><i>[Facility*8][Severity]</i></p> <p>Event/alert severity values are as follows:</p> <ul style="list-style-type: none"> • Critical = 2 • Warning = 4 • Informational = 6
Location field	(Optional) Enter location information (up to 29 characters). This information will be populated in the syslog message.
Hostname editable column	Enter an IP address or DNS name for the host.
Port editable column	<p>Enter a port number on which the syslog daemon is listening. If the port number is left unspecified (empty), the port defaults to 514.</p> <p>Note The syslog daemon on the remote system (hostname) must be configured to listen on a specified port.</p>
Comments editable column	(Optional) A comment.

Step 6 Click **Next**. The Notification Group Summary page appears, displaying all information entered on the previous page.

Step 7 Click **Finish**. The notification information is saved.

Adding and Editing Service Quality Notification Groups

This section describes the procedures for adding or editing a service quality notification group.



Note

You can use existing notification groups as templates for creating new notification groups. For procedures, see [Cloning a Notification Group, page 14-17](#).

Step 1 Select **Notifications > Notification Criteria**.

Step 2 Do one of the following:

- To add a new group, click **Add > Service Quality-Based Criterion**.
- To edit an existing group, select the check box next to a service quality notification group and click **Edit**.

Depending on your selection, the Add Service Quality-Based Criterion page or Edit Service Quality-Based Criterion page appears.

Step 3 Edit the information on the page, described in the following table.

GUI Element	Description/Action
Notification Criterion field	Enter a name for the notification criterion.
Destination fields	<p>(Optional). To generate notifications for alerts and events on call destinations, do the following:</p> <ol style="list-style-type: none"> 1. Select an operator (Is Exactly, Contains, Begins With, Any). 2. Enter an appropriate value: Phone extension or IP address for an endpoint, such as a voice gateway or a phone.
Source fields	<p>(Optional). To generate notifications for alerts and events on call sources, do the following:</p> <ol style="list-style-type: none"> 1. Select an operator (Is Exactly, Contains, Begins With, Any). 2. Enter an appropriate value: Phone extension or IP address for a voice gateway or a phone.
Cisco 1040 ID fields	<p>(Optional). To generate notifications for alerts and events on particular Cisco 1040s, do the following:</p> <ol style="list-style-type: none"> 1. Select an operator (Is Exactly, Contains, Begins With, Any). 2. Enter the ID for a Cisco 1040. These typically start with a letter followed by 3 digits, for example <i>A100</i>.
Phone Model list	<p>(Optional). To generate notifications for alerts and events on particular phone models, enter a comma-separated list of Cisco IP phone models or select them from a list:</p> <ol style="list-style-type: none"> 1. Click the icon to open a selector. 2. Select a phone model from the list. To select more than one phone model, hold down Ctrl while selecting. 3. Click OK.
Alert Severity check boxes	<p>Select any:</p> <ul style="list-style-type: none"> • Critical. • Warning. • Informational.
Alert Status check boxes	<p>Select any:</p> <ul style="list-style-type: none"> • Active. • Cleared.
Event Severity check boxes	<p>Select any:</p> <ul style="list-style-type: none"> • Critical. • Warning. • Informational.

GUI Element	Description/Action
Event Status check boxes	Select any: <ul style="list-style-type: none"> • Active. • Cleared. For more information about event status, see Using the Service Quality Alert Details Display, page 4-7 .
Event Description check boxes	Select any: <ul style="list-style-type: none"> • Service Quality Issue. • Critical Service Quality Issue. • Multiple Service Quality Issues. • Cisco 1040 Sensor Down. Note For more information about these events, see Events Processed, page D-1 .
Cause check boxes	Select any: <ul style="list-style-type: none"> • Jitter. • Latency.

Step 4 Click **Next**. The Destination: Edit Qov Criteria page appears.

Step 5 Edit the information on this page as described in the following table.

GUI Element	Description/Action
Always Active check box	Schedules the notification group to always be active.
Active From: To: fields	Select the hours of the day during which you want this subscription to be active: <ul style="list-style-type: none"> • From: HH:MM—Select hour and minute that the subscription becomes active. • To: HH:MM—Select the last hour and minute during which the subscription is active. By default, the values are from 00:00 to 00:00 and the subscription is active for 24 hours. Note Use this field, for example, to send e-mail notifications to a pager during one shift and not during another.
Include Link to Notification Details check box	Select to include URLs in the notification from which users can directly open the relevant page in Operations Manager for more information. Deselect to omit URLs from notifications.

GUI Element	Description/Action
Subscription Type radio buttons	<p>Select one at a time to enter data for each subscription type that you want to include in this subscription:</p> <ul style="list-style-type: none"> Trap—Enter data in the Trap Subscription Type fields, page 14-16. E-Mail—Enter data in the E-Mail Subscription Type fields, page 14-16. Syslog—Enter data in the Syslog Subscription Type fields, page 14-16. <p>Note Operations Manager does not save the data you enter until you click Finish on the Subscription: Summary page. To go to the Subscription: Summary page, click Next.</p>
Trap Subscription Type fields	
Hostname editable column	Enter an IP address or DNS name for the host.
Port editable column	Enter a port number on which the host can receive traps. If the port number is left unspecified (empty), the port defaults to 162.
Comments editable column	(Optional) Enter a comment.
E-Mail Subscription Type fields	
SMTP Server field	<p>Enter a fully qualified DNS name or IP address for a Simple Mail Transfer Protocol (SMTP) server. (The name of the default SMTP server might already be displayed.)</p> <p>Note To select from any nondefault SMTP servers in use by existing subscriptions, click the SMTP Servers button.</p> <p>Note For instructions on how to configure a default SMTP server, see the Setting System-Wide Parameters Using System Preferences, page 19-12.</p>
Sender Address field	Enter the e-mail address that notifications should be sent from. If the sender's e-mail service is hosted on the SMTP server specified, you need enter only the username. You do not need to enter the domain name.
Recipient Address(es) field	<p>Enter one or more e-mail addresses that notifications should be sent to, separating multiple addresses with either a comma or a semicolon.</p> <p>If a recipient's e-mail service is hosted on the SMTP server specified, you need to enter only the username. You do not need to enter the domain name.</p>
Subject Only check box	<p>Select to include only the subject in the e-mail message.</p> <p>Deselect to send a fully detailed e-mail message (default).</p>
Syslog Subscription Type fields	

GUI Element	Description/Action
Facility list	<p>Select a facility from the list (the default is Local Use 0). The Facility field and the event/alert severity are used for the PRI portion of the syslog message, as follows:</p> <p style="text-align: center;"><i>[Facility*8][Severity]</i></p> <p>Event/alert severity values are as follows:</p> <ul style="list-style-type: none"> • Critical = 2 • Warning = 4 • Informational = 6
Location field	(Optional) Enter location information (up to 29 characters). This information will be populated in the syslog message.
Hostname editable column	Enter an IP address or DNS name for the host.
Port editable column	<p>Enter a port number on which the syslog daemon is listening. If the port number is left unspecified (empty), the port defaults to 514.</p> <p>Note The syslog daemon on the remote system (hostname) must be configured to listen on a specified port.</p>
Comments editable column	(Optional) A comment.

Step 6 Click **Next**. The Notification Group Summary page appears, displaying all information entered on the previous page.

Step 7 Click **Finish**. The notification information is saved.

Cloning a Notification Group

You can use existing notification groups as templates for creating new notification groups.

Step 1 Select **Notifications > Notification Criteria**. The Notification Groups page appears.

Step 2 Select the check box next to the notification group that you want to use as the base for your new notification group.

Step 3 Click **Clone**. Depending on your selection, the Clone Device-Based Criterion page or the Clone Service Quality-Based Criterion page appears.

The rest of the procedures for cloning a notification group are the same as when a notification group is edited. For further instructions, see the following:

- [Adding and Editing Device Notification Groups, page 14-10](#)
- [Adding and Editing Service Quality Notification Groups, page 14-13](#)

Viewing Notification Group Configuration Details

-
- Step 1** Select **Notifications > Notification Criteria**. The Notification Groups page appears.
- Step 2** Select the check box next to a notification group.
- Step 3** Click **View**. The Notification Group Summary page appears, displaying the following information:
- Notification Name.
 - Notification Group Details—Alert, event, and device type information.
 - Destination Details—Trap, e-mail, or syslog destination information.
-

Deleting Device or Service Quality Notification Groups

-
- Step 1** Select **Notifications > Notification Criteria**. The Notification Groups page appears.
- Step 2** Select the check box next to each notification group that you want to delete.
- Step 3** Click **Delete**. A confirmation dialog box appears.
- Step 4** Click **Yes** to confirm.
-

Suspending a Notification

After you suspend a notification, Operations Manager stops using it until you resume it (see [Resuming a Notification](#), page 14-19).

You can suspend a subscription and resume it at any time. You can also schedule a period during the day when you want a notification to be active. For more information, see [Adding and Editing Device Notification Groups](#), page 14-10.

**Note**

After suspending a notification, the suspend button may still appear enabled. You cannot suspend an already suspended notification. Clicking the Suspend button will have no effect on the notification. You should use the Notification Groups page to determine the status of a notification.

Use this procedure to suspend any type of notification: e-mail, SNMP trap, or syslog.

- Step 5** Select **Notifications > Notification Criteria**. The Notifications Group page appears. Select the check box next to each notification group that you want to suspend.
- Step 6** Click **Suspend**. A confirmation dialog box appears.
- Step 7** Click **Yes** to confirm.
-

Resuming a Notification

You can resume a notification when its status is Suspended. After resuming a notification it will go into either active or inactive state depending on the time at which the notification group is resumed, and the time of day settings for that notification group.

Resuming a notification group does not override its time of day settings. The group will resume to operate as it did before suspension.

**Note**

You can resume a notification group only after it has been suspended (it is in the Suspended state). You cannot resume a notification group during its inactive time (it is in the Inactive state), even if the Resume button is enabled.

Use this procedure to resume a suspended notification of any type: e-mail, SNMP trap, or syslog.

-
- Step 1** Select **Notifications > Notification Criteria**. The Notification Group page appears. Select the check box next to each notification group that you want to resume.
- Step 2** Click **Resume**. A confirmation dialog box appears.
- Step 3** Click **Yes** to confirm.
-

Customizing Events

You can customize event description and event severity for any event that is displayed in Operations Manager.

Customizing events is described in the following sections:

- [Where Customized Event Descriptions Are Displayed, page 14-19](#)
- [Where Customized Event Severity Is Displayed, page 14-20](#)
- [Customizing Event Description and Severity, page 14-20](#)
- [Restoring Default Event Descriptions and Severities, page 14-21](#)

Where Customized Event Descriptions Are Displayed

When you customize an event description, the new description is reflected in all notifications—e-mail, SNMP traps, and syslog—and on all user interfaces. For example, customized event descriptions are displayed on the Alert Details page and in Alert History and Event History reports.

Where Customized Event Severity Is Displayed

When you customize event severity, it is reflected in all notifications—e-mail, SNMP traps, and syslog. Operations Manager uses only the event severity levels in the following table.

Table 14-3 *Event Severity Levels and Values that Operations Manager Uses*

Severity Level	Value that Operations Manager Defines	Value That Operations Manager Writes to Notifications	
		E-Mail and SNMP Traps	Syslog Messages
Critical	0	0	2
Warning	1	1	4
Informational	2	2	6

You can specify a customized event severity level between 0 and 7. When generating traps, the severity level you specify for the event is stored in the CISCO-EPM-NOTIFICATION-MIB and is sent in all notifications.



Note

When you customize event severity, Operations Manager continues to process the event based on its default severity. Also, severity levels 3 through 7 are undefined in Operations Manager.

You can quickly and easily restore the default name and severity for any and all events.

Customizing Event Description and Severity



Note

Default event names are displayed on the Event Customization page. For default event severity, locate the event in [Events Processed, page D-1](#).

Step 1

Select **Notifications > Event Customization**. The Event Customization page appears, displaying the information shown in the following table.

GUI Element	Description/Action
Number column	Numbers events serially from one.
Check box column	Select to customize an event.
Event Code column	Code number for the event. This number cannot be changed and is used to map default names to customized names.
Default Description column	Default description for the event. This description is not editable.

GUI Element	Description/Action
Current Description column	This is an editable field. For more information, see Where Customized Event Descriptions Are Displayed, page 14-19 .
Current Severity column	Select a severity for the event. For more information, see Where Customized Event Severity Is Displayed, page 14-20 . Note For default event severity levels, locate the event in Events Processed, page D-1 .

- Step 2** For each event that you want to customize:
- Select the check box.
 - Enter any changes in the following fields:
 - New Description**—Enter a new description.
 - New Severity**—Select a new severity level from 0 to 7.
- Step 3** Click **OK** to save your changes and apply them.

For additional information, please see the following topics:

- [Getting Alert and Event Details, page 3-9](#)
- [Events Processed, page D-1](#)

Restoring Default Event Descriptions and Severities

- Step 1** Select **Notifications > Event Customization**. The Notification Customization page appears, displaying the information shown in the following table.

GUI Element	Description/Action
Number column	Numbers events serially from one.
Check box column	Select: <ul style="list-style-type: none"> The topmost check box to restore default description and severity to all events. One or more check boxes in rows with events that you want restored to default description and default severity.
Event Code column	Code number for the event. This number cannot be changed and is used to map default names to customized names.
Default Description column	Default description for the event. This description is not editable.

GUI Element	Description/Action
Current Description column	This is an editable field. However, you do not need to enter any changes to restore the default description.
Current Severity column	This is an editable field. However, you do not need to select a value to restore the default severity. Note For default event severity levels, locate the event in Events Processed, page D-1 .

- Step 2** Select the check box for all events or select multiple check boxes for the events that you want to restore to default description and severity.
- Step 3** Click **Restore Default Description**.
- Step 4** Apply your changes by clicking **Yes** when the confirmation window appears.

For additional information, please see the following topics:

- [Getting Alert and Event Details, page 3-9](#)
- [Events Processed, page D-1](#)